Monero's Building Blocks
Part 6 of 10 – *Linkable Spontaneous Anonymous Group (LSAG) signature scheme*

Bassam El Khoury Seguias

BTC: 3FcVvBZwTUkUrcqJd16RcjR42qT2tDWHWn

ETH: 0xb79Fb9194C8Cc6221368bb70976e18609Ab9AcA8

March 29, 2018

1 Introduction

For a given ring size n, Cryptonote's original scheme (as introduced in part 5), generates signatures of the form $(I, c_1, .., c_n, r_1, .., r_n)$ consisting of $(2n+1)$ arguments. It turns out that a more efficient scheme initially introduce in [3] and later adapted by Adam Back in [1] can achieve the same security properties as Cryptonote's with $(n+2)$ arguments instead (a reduction factor that tends to 2 as n tends to ∞). The scheme introduced in [3] is known as *Linkable Spontaneous Anonymous Group* signature or LSAG for short. In part 7 of this series, we will see how [4] generalizes the LSAG construct to build the foundation of Monero's current *ringCT* signature scheme.

2 The LSAG scheme

The LSAG signature introduced in [3] is built on a group E of prime order q and generator G. Moreover, it uses 2 statistically independent ROs:

- $\mathcal{H}_1 : \{0,1\}^* \longrightarrow \mathbb{F}_q$
- $\mathcal{H}_2 : \{0,1\}^* \longrightarrow E$

In what follows we introduce a slightly modified LSAG scheme that will allow an easier comparison to Cryptonote's original scheme. We carry forward all the notation used in the Cryptonote scheme to the current LSAG definition. In particular, we let E be a large finite group generated by the same elliptic curve introduced in part 5 (refer to the post entitled *Elliptic Curve Groups* for an introduction to the topic). The curve's equation is given by:

$$E : -x^2 + y^2 = 1 + dx^2y^2$$

As described in part 5, the above equation is a polynomial over $\mathbb{F}_q$ where q is a very large prime and d is a pre-defined element of $\mathbb{F}_q$. We simplify the notation and refer to the group generated by this elliptic curve as $E(\mathbb{F}_q)$. We recall below what we observed in part 5:

- Elements of $E(\mathbb{F}_q)$ are pairs $(x, y) \in \mathbb{F}_q^2$ that satisfy the above equation.
- Elliptic curve groups in general and $E(\mathbb{F}_q)$ in particular have a well defined addition operation that we denote by $\oplus$.
- $E(\mathbb{F}_q)$ contains a special element G (not necessarily unique) that we refer to as the base point. The base point has order $l < q$, where l is a very large prime. That means that adding G to itself l times yields the identity element e of $E(\mathbb{F}_q)$. In other terms, $G \oplus ... \oplus G = e$. We simply write $l \otimes G = e$ (the notation $\otimes$ serves as a reminder that this is scalar multiplication associated with $\oplus$).
- We let $\{G\}$ denote the group generated by G under the $\oplus$ operation of $E(\mathbb{F}_q)$. We also let $\{G\}^* \equiv \{G\} - e$.
- Solving the Discrete Logarithm (DL) problem on $\{G\}^*$ (and more generally on $E(\mathbb{F}_q)$) is thought to be intractable.

With a slight divergence from [3], we first introduce a hash function $\mathcal{H}_T$ before we define $\mathcal{H}_2$. The reason will become clearer in section 4 when we build the signing simulator to prove LSAG's resilience against EFACM.

- $\mathcal{H}_1 : \{0,1\}^* \longrightarrow \mathbb{F}_q$
- $\mathcal{H}_T : \{G\}^* \longrightarrow \mathbb{F}_l^* \times \{G\}^*$

  $\mathcal{H}_T$ takes an element $s \in \{G\}^*$ and outputs a tuple $(v_s, v_s \otimes G) \in \mathbb{F}_l^* \times \{G\}^*$. Here v_s is a random element chosen according to a uniform distribution over $\mathbb{F}_l^*$. We then let $\mathcal{H}_2(s) \equiv v_s \otimes G$. So $\mathcal{H}_2 : \{G\}^* \longrightarrow \{G\}^*$, takes an element $s \in \{G\}^*$ and returns an element $v_s \otimes G \in \{G\}^*$ where v_s is randomly chosen in $\mathbb{F}_l^*$.

  Note that [3] defines $\mathcal{H}_2$ as a map from $\{0,1\}^*$ to $E \equiv E(\mathbb{F}_q)$. Here we restricted the domain and the range to $\{G\}^*$ instead. This is because in this version of LSAG, $\mathcal{H}_2$ is strictly applied to public keys as opposed to any element of $\{0,1\}^*$. Public keys are elements of $E(\mathbb{F}_q)$ that are scalar multiples of the base point G. Moreover, the scalar is never equal to order$(G) = l$ (we impose this constraint when we introduce the key generation algorithm $\mathcal{G}$). We are then justified in restricting the domain to $\{G\}^*$. The range is arbitrarily defined to be $\{G\}^*$, which is permissible since it preserves the injective nature of the map.

The scheme is defined by a set of 4 algorithms:

- **The key generation algorithm** $\mathcal{G}$. On input 1^k (k is the security parameter that by design we request to satisfy $k < log_2|\{G\}^*| = log_2(l-1)$), it produces a pair $(sk, pk) \equiv (x, y)$ of matching secret and public keys. x is randomly chosen in $\mathbb{F}_l^* \equiv \{1, ..., l-1\}$, and y is calculated as $x \otimes G$. (Note that G and y are both elements of $\{G\}^* \subset EC(\mathbb{F}_q)$ while x is an element of $\mathbb{F}_l^* \subset \mathbb{F}_q$.

In addition to the (x, y) key pair, $\mathcal{G}$ computes $I \equiv x \otimes \mathcal{H}_2(y)$. I is known as the *key image* (or *tag*). It is signer-specific since it depends only on the signer's private and public keys. It allows the ring linkability algorithm $\mathcal{L}$ to test for independence between different signatures. $\mathcal{G}$ is modeled as a PPT Turing machine. We observe that in [3], the key-image or tag is computed as part of the ring signing algorithm Σ as opposed to $\mathcal{G}$. We include it in $\mathcal{G}$ to ensure consistency with Cryptonote's original construct.

- **The ring signing algorithm** Σ. Suppose a user A_π decides to sign a message m on behalf of the ring of users $L \equiv \{A_1, ..., A_n\} \ni A_\pi$. A_π has a key pair given by (x_π, y_π) and a key-image (or tag) given by $I_\pi \equiv x_\pi \otimes \mathcal{H}_2(y_\pi)$. Σ does the following:

  1. Choose random $q_\pi \in \{1, ..., l\} \equiv \mathbb{F}_l$. Assign:

     $\{\ L_\pi \equiv (q_\pi \otimes G)$
     $\{\ R_\pi \equiv (q_\pi \otimes \mathcal{H}_2(y_\pi))$
     $\{\ c_{\pi+1} \equiv \mathcal{H}_1(m, L_\pi, R_\pi) \pmod{l}$

  2. $\forall i \in \{\pi + 1, .., n, 1, .., \pi - 1\}$, choose random $r_i \in \{1, ...l\} \equiv \mathbb{F}_l$. Assign:

     $\{\ L_i \equiv (r_i \otimes G) \ \oplus \ (c_i \otimes y_i)$
     $\{\ R_i \equiv (r_i \otimes \mathcal{H}_2(y_i)) \ \oplus \ (c_i \otimes I_\pi)$
     $\{\ c_{i+1} \equiv \mathcal{H}_1(m, L_i, R_i) \pmod{l}$

     where $c_{n+1} \equiv c_1$

  3. Set $r_\pi \equiv q_\pi - c_\pi x_\pi \pmod{l}$. Here $c_\pi x_\pi$ denotes regular scalar multiplication in modulo l arithmetic.

  Σ outputs a signature $\sigma_\pi(m, L) \equiv (I_\pi, c_1, r_1, .., r_n)$. Σ is a PPT algorithm.

- **The ring verification algorithm** $\mathcal{V}$. Given a ring signature σ, a message m, and the set $\{y_1, .., y_n\}$ of public keys of the ring members:

  - *(Verification equations #1 to #3n)*: let $c'_1 = c_1$. $\forall i \in \{1, ..., n\}, \mathcal{V}$ assigns

    $\{\ L'_i \equiv (r_i \otimes G) \ \oplus \ (c'_i \otimes y_i)$
    $\{\ R'_i \equiv (r_i \otimes \mathcal{H}_2(y_i)) \ \oplus \ (c'_i \otimes I_\pi)$
    $\{\ c'_{i+1} \equiv \mathcal{H}_1(m, L'_i, R'_i) \pmod{l}$

  - *(Verification equation #(3n + 1))*: $\mathcal{V}$ checks whether

    $\{\ c_1 = c'_{n+1}$, where $c'_{n+1} \equiv \mathcal{H}_1(m, L'_n, R'_n) \pmod{l}$

  If equality holds, the signature is valid and $\mathcal{V}$ outputs *True*. Otherwise, it outputs *False*. $\mathcal{V}$ is a deterministic algorithm.

- **The ring linkability algorithm** $\mathcal{L}$. It takes a $\mathcal{V}$-verified valid signature $\sigma_\pi(m, L)$. It checks if the key-image I_π was used in the past by comparing it to previous key-images stored in a set $\mathcal{I}$. If a match is found, then with overwhelming probability the 2 signatures were produced by the same key pair (as will be justified when we prove the *exculpability* of LSAG in section 5 below), and

$\mathcal{L}$ outputs *Linked*. Otherwise, its key-image is added to $\mathcal{I}$ and $\mathcal{L}$ outputs *Independent*.

3 Security analysis - Correctness

Let $\sigma_\pi(m, L) \equiv (I_\pi, c_1, r_1, ..., r_n)$ be a Σ-generated signature. Without loss of generality, assume $1 < \pi \leq n$. Then $\forall i, 1 \leq i < \pi$, we have the following implication:

If $\{(c'_i = c_i) \cap (L'_i = L_i) \cap (R'_i = R_i)\}$, then:

$$\{ \ c'_{i+1} = \mathcal{H}_1(m, L'_i, R'_i) \pmod{l} = \mathcal{H}_1(m, L_i, R_i) \pmod{l} = c_{i+1}$$

$$\{ \ L'_{i+1} \equiv (r_{i+1} \otimes G) \oplus (c'_{i+1} \otimes y_{i+1}) = (r_{i+1} \otimes G) \oplus (c_{i+1} \otimes y_{i+1}) = L_{i+1}$$

$$\{ \ R'_{i+1} \equiv (r_{i+1} \otimes \mathcal{H}_2(y_{i+1})) \oplus (c'_{i+1} \otimes I_\pi) = (r_{i+1} \otimes \mathcal{H}_2(y_{i+1})) \oplus (c_{i+1} \otimes I_\pi) = R_{i+1}$$

Recall that $c'_1 = c_1$ (by design of $\mathcal{V}$) and so $L'_1 = L_1$ and $R'_1 = R_1$. We therefore conclude by induction on c'_i that $\forall i \ 1 \leq i \leq \pi$, $c'_i = c_i$. In particular, $c'_\pi = c_\pi$. This implies:

$$\{ \ L'_\pi = (r_\pi \otimes G) \oplus (c'_\pi \otimes y_\pi) = ((q_\pi - c_\pi x_\pi) \otimes G) \oplus (c_\pi \otimes y_\pi) = q_\pi \otimes G = L_\pi$$

$$\{ \ R'_\pi = (r_\pi \otimes \mathcal{H}_2(y_\pi)) \oplus (c'_\pi \otimes I_\pi) = ((q_\pi - c_\pi x_\pi) \otimes \mathcal{H}_2(y_\pi)) \oplus (c_\pi \otimes I_\pi) = q_\pi \otimes \mathcal{H}_2(y_\pi) = R_\pi$$

We can then invoke a similar induction argument on c'_i as the one stated earlier, but this time for $\pi \leq i \leq n$. We therefore conclude that:

$$c_1 \equiv c_{n+1} \equiv \mathcal{H}_1(m, L_n, R_n) \pmod{l} \textit{ (by design of } \Sigma\textit{)}$$

$$= \mathcal{H}_1(m, L'_n, R'_n) \pmod{l} \textit{ (by induction proof showing that } L'_n = L_n \textit{ and } R'_n = R_n\textit{)}$$

Subsequently, any Σ-generated signature will satisfy $\mathcal{V}$'s verification test.

4 Security analysis - Unforgeability vis-a-vis EFACM

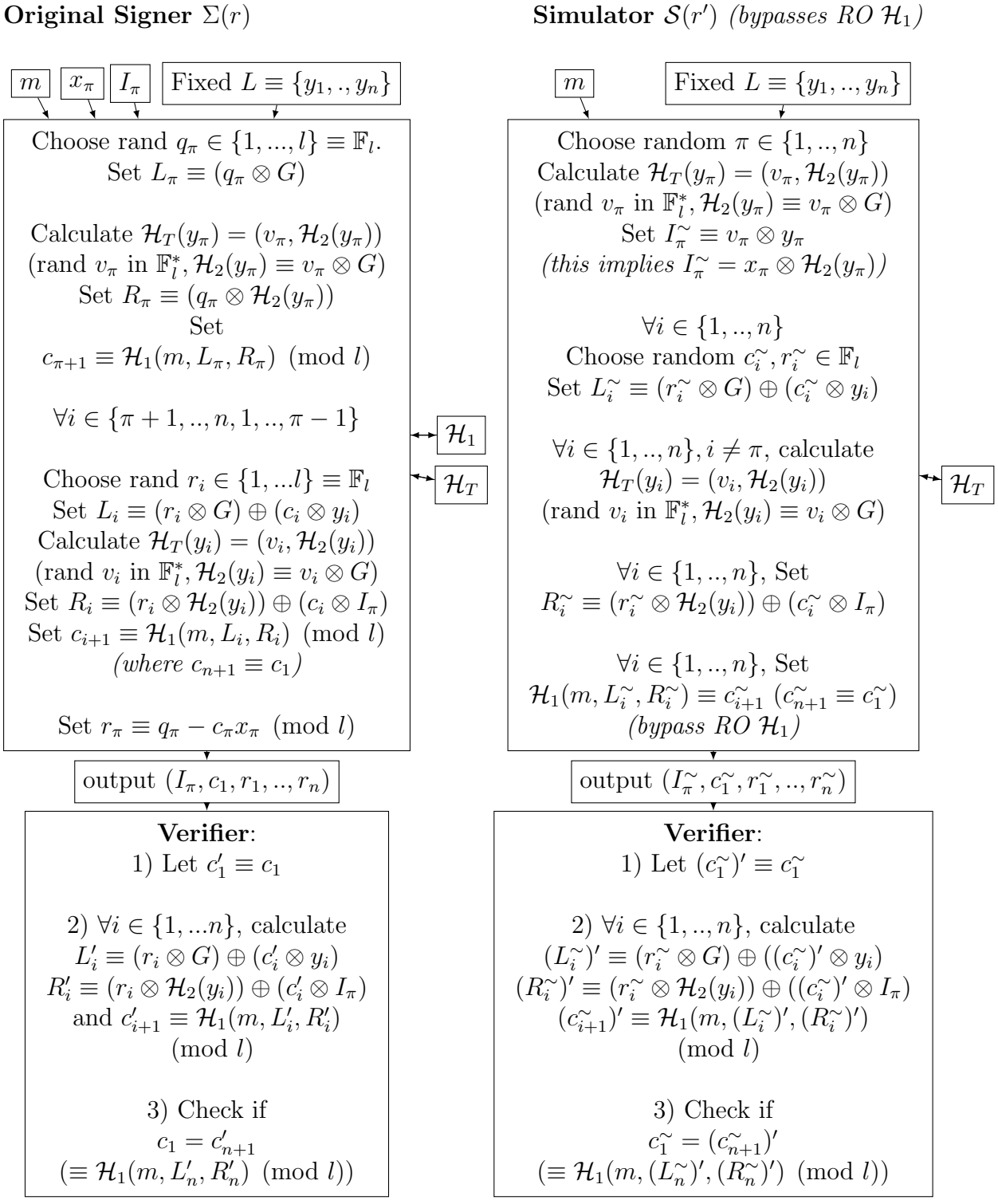
For unforgeability proofs, we follow the 5-step approach outlined earlier in part 1. (Recall that for ring signatures, we prove resilience against EFACM with respect to a fixed ring attack as described in part 3 of this series).

Step 1 : To prove that this scheme is secure against EFACM in the RO model, we proceed by contradiction and assume that there exists a PPT adversary $\mathcal{A}$ such that:

$$P_{\omega,r,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\Sigma^{\mathcal{H}_1,\mathcal{H}_T}(r)} \textit{ succeeds in } EFACM] = \epsilon(k), \text{ for } \epsilon \text{ non-negligible in } k.$$

Step 2 : Next, we build a simulator $\mathcal{S}(r')$ such that it:

- Does not have access to the private key of any signer.
- Has the same range as the original signing algorithm Σ (i.e., they output signatures taken from the same pool of potential signatures over all possible choices of RO functions and random tapes r' and r).
- Has indistinguishable probability distribution from that of Σ over this range.



The reason we introduced $\mathcal{H}_T$ as opposed to introducing only $\mathcal{H}_2$ is that the simulator makes use of the random element v_π in order to set $I_\pi^\sim$ to the desired value. In other words, the simulator needs to have access to the random element $v_\pi \in \mathbb{F}_l^*$ that is used in the calculation of $\mathcal{H}_2(y_\pi)$ in order to ensure that $I_\pi^\sim$ equates to $x_\pi \otimes \mathcal{H}_2(y_\pi)$.

By construction, the output of $\mathcal{S}$ will satisfy the verification equation. Moreover, it does its own random assignments to what otherwise would be calls to RO $\mathcal{H}_1$ (i.e., S bypasses RO $\mathcal{H}_1$). Next, note the following:

1. $\mathcal{S}$ does not use any private key.
2. Σ and $\mathcal{S}$ both have a range $R \equiv \{(\gamma, \epsilon_1, \beta_1, ..., \beta_n) \in \{G\}^* \times (\mathbb{F}_l)^{n+1}$ such that $\epsilon_1 = \mathcal{H}_1(m, L'_n, R'_n) \pmod l$ and where L'_n and R'_n are calculated as follows:
   - Let $c'_1 \equiv \epsilon_1$
   - $\forall i \in \{1, .., n\}$, compute:
     $\{\ L'_i = (\beta_i \otimes G) \oplus (c'_i \otimes y_i)$
     $\{\ R'_i = (\beta_i \otimes \mathcal{H}_2(y_i)) \oplus (c'_i \otimes \gamma)$
     $\{\ c'_{i+1} = \mathcal{H}_1(m, L'_i, R'_i)$
3. Σ and $\mathcal{S}$ have the same probability distribution over R. Indeed, $\forall(\gamma, \epsilon_1, \beta_1, .., \beta_n) \in R$, we have:
   - For Σ :

$$P[(I_\pi, c_1, r_1, .., r_n) = (\gamma, \epsilon_1, \beta_1, ..., \beta_n)] =$$

$$P_{I_\pi \in \{G\}^*,\ c_1 \in \mathbb{F}_l,\ r_i \in \mathbb{F}_l}[(I_\pi = \gamma)\ \cap\ (c_1 = \epsilon_1)\ \cap\ (r_i = \beta_i,\ \forall i \in \{1, ..., n\})]$$

$$= \tfrac{1}{|\{G\}^*|} \times (\tfrac{1}{l})^{n+1} = \tfrac{1}{(l-1)\times l^{n+1}}$$

     The first factor is the probability of choosing the exact I_π value in the set $\{G\}^*$ that is equal to γ. The second factor is the probability of choosing the exact $n+1$ values given by ϵ_1 and the β_i's $\in \mathbb{F}_l$.

   - For $\mathcal{S}$:

$$P[(I_\pi^\sim, c_1^\sim, r_1^\sim, .., r_n^\sim) = (\gamma, \epsilon_1, \beta_1, ..., \beta_n)] =$$

$$P_{I_\pi^\sim \in \{G\}^*,\ c_1^\sim \in \mathbb{F}_l,\ r_i^\sim \in \mathbb{F}_l}[(I_\pi^\sim = \gamma)\ \cap\ (c_1^\sim = \epsilon_1)\ \cap\ (r_i^\sim = \beta_i,\ \forall i \in \{1, ..., n\})]$$

$$= \tfrac{1}{|\{G\}^*|} \times (\tfrac{1}{l})^{n+1} = \tfrac{1}{(l-1)\times l^{n+1}}$$

     Note that the range of $I_\pi^\sim$ is equal to $\{G\}^*$ by construction of S. And so the first factor is the probability of choosing the exact $I_\pi^\sim$ value in the set $\{G\}^*$ that is equal to γ. The second factor is the probability of choosing the exact $n+1$ values given by ϵ_1 and the β_i's $\in \mathbb{F}_l$.

With $\mathcal{S}$ adequately built, we conclude that (refer to section 6 of part 1 of this series for a justification):

$$P_{\omega,r,'\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\mathcal{S}^{\mathcal{H}_T}(r')} \textit{ succeeds in } EFACM] = \epsilon(k), \text{ for } \epsilon \text{ non-negligible in } k.$$

Step 3 : We now show that the probability of faulty collisions is negligible (refer to section 6 of part 1 of this series for an overview). The 2 tyes of collisions are:

- $Col_{Type\ 1}$: there exists $i \in \{1,..,n\}$ such that a tuple (m, L_i, R_i) that $\mathcal{S}$ encounters – recall that $\mathcal{S}$ makes its own random assignment to $\mathcal{H}_1(m, L_i, R_i)$ and bypasses RO $\mathcal{H}_1$ – also appears in the list of queries that $\mathcal{A}(\omega)$ sends to RO $\mathcal{H}_1$. A conflict in the 2 values will happen with overwhelming probability and the execution will halt.
- $Col_{Type\ 2}$: there exists $i, j \in \{1,..,n\}$ such that a tuple (m, L_i, R_i) that $\mathcal{S}$ encounters – recall that $\mathcal{S}$ makes its own random assignment to $\mathcal{H}_1(m, L_i, R_i)$ – is the same as another tuple (m', L'_j, R'_j) that $\mathcal{S}$ encountered earlier – here too, $\mathcal{S}$ would have made its random assignment to $\mathcal{H}_1(m', L'_j, R'_j)$. Since the tuples are identical (i.e., $(m, L_i, R_i) = (m', L'_j, R'_j)$), the assignments must match (i.e., $\mathcal{H}_1(m, L_i, R_i) = \mathcal{H}_1(m', L'_j, R'_j)$). However, the likelihood that the 2 are equal is negligible. Hence they will be different with overwhelming probability and the execution will halt.

The aforementioned collisions must be avoided. In order to do so, we first calculate the probability of their occurence. We assume that during an EFACM attack, $\mathcal{A}(\omega)$ can make a maximum of Q_1 queries to RO $\mathcal{H}_1$, a maximum of Q_T queries to RO $\mathcal{H}_T$, and a maximum of Q_S queries to $\mathcal{S}(r')$. Q_1, Q_T, and Q_S are all assumed to be polynomial in the security parameter k, since the adversary is modeled as a PPT Turing machine.

$$P[Col_{Type\ 1}] = P[\cup_{all\ (m,L_i,R_i),\ (i=1,..,n)}\{(m, L_i, R_i) \textit{ appeared in at least one of the } Q_S \textit{ queries to } \mathcal{S} \textit{ and } Q_1 \textit{ queries to RO } \mathcal{H}_1\}]$$

$$\leq \sum_{i=1}^{n} P[\cup_{all\ L_i}\{L_i \textit{ was part of at least one of the } Q_S \textit{ queries to } \mathcal{S} \textit{ and } Q_1 \textit{ queries to RO } \mathcal{H}_1\}]$$

$$\leq \sum_{i=1}^{n} \sum_{all\ L_i \in \{G\}} P[\cup_{(j=1,..,Q_S),\ (k=1,..,Q_1)}\{L_i \textit{ was part of at least the } j^{th} \textit{ query to } \mathcal{S} \textit{ and } k^{th} \textit{ queries to RO } \mathcal{H}_1\}]$$

$$\leq \sum_{i=1}^{n} \sum_{all\ L_i \in \{G\}} \sum_{j=1}^{Q_S} \sum_{k=1}^{Q_1} P[L_1 \textit{ was part of at least the } j^{th} \textit{ query to } \mathcal{S} \textit{ and } k^{th} \textit{ queries to RO } \mathcal{H}_1]$$

$$\leq \sum_{i=1}^{n} \sum_{all\ L_i \in \{G\}} \sum_{j=1}^{Q_S} \sum_{k=1}^{Q_1} \frac{1}{|\{G\}|^2} = n \times |\{G\}| \times \frac{Q_S Q_1}{|\{G\}|^2} = n \times \frac{Q_S Q_1}{|\{G\}|} < \frac{n Q_S Q_1}{2^k}.$$

$$(\textit{since } k < log_2(|\{G\}^*|) < log_2(|\{G\}|) \textit{ by design}).$$

Recalling that Q_S and Q_1 are polynomial in k, we conclude that $P[Col_{Type\ 1}]$ is negligible in k.

Next, we compute $P[Col_{Type\ 2}] =$

$$P[\cup_{all\ (m,L_i,R_i),\ (i=1,..,n)}\{(m,L_i,R_i)\ appeared\ at\ least\ twice\ during\ queries\ to\ \mathcal{S}\}]$$

$$\leq \sum_{i=1}^{n} P[\cup_{all\ L_i\in\{G\}}\{L_i\ was\ part\ of\ at\ least\ 2\ queries\ to\ \mathcal{S}\}]$$

$$\leq \sum_{i=1}^{n}\sum_{L_i\in\{G\}}\binom{Q_S}{2}\times\frac{1}{|\{G\}|^2} < n\times|\{G\}|\times\binom{Q_S}{2}\times\frac{1}{|\{G\}|^2} < n\times\binom{Q_S}{2}\times\frac{1}{|\{G\}|} < \frac{nQ_S^2}{2\times 2^k}.$$

$$(\text{since } k < log_2(|\{G\}^*|) < log_2(|\{G\}|) \text{ by design}).$$

Recalling that Q_S is polynomial in k, we conclude that $P[Col_{Type\ 2}]$ is negligible in k.

Putting it altogether, we find that the below quantity is negligible in k:

$$P[Col] = P[Col_{Type\ 1}\cup Col_{Type\ 2}] \leq \sum_{i=1}^{2} P[Col_{Type\ i}] \leq n(\frac{Q_S Q_1+\frac{Q_S^2}{2}}{2^k}) \equiv \delta(k)$$

This allows us to conclude that the below quantity is non-negligible in k (refer to section 6 of part 1 for a justification):

$$P_{\omega,r,'\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\mathcal{S}^{\mathcal{H}_T(r')}} succeeds\ in\ EFACM\ \cap\overline{Col}] \geq \epsilon(k)-\delta(k).$$

Step 4 : In this step, our objective is to show that if $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$ is a successful tuple that generated a first EFACM forgery, then the following quantity is non-negligible in k:

$$P_{\mathcal{H}_1}[\mathcal{A}(\omega^*)^{\mathcal{H}_1,\mathcal{H}_T^*,\mathcal{S}^{\mathcal{H}_T(r'^*)}}\ succeeds\ in\ EFACM\ \cap\ (\rho_{\alpha(\mu_{\vec{\beta}})}\neq\rho^*_{\alpha(\mu_{\vec{\beta}})})\ |$$
$$(\omega^*,r'^*,\mathcal{H}_1^*,\mathcal{H}_T^*)\ is\ a\ succesfull\ first\ forgery,\ and\ (\rho_i=\rho_i^*)\ for\ i\in\{1,...\alpha(\mu_{\vec{\beta}})-1\}]$$

Here $\alpha(\mu_{\vec{\beta}})$ is an appropriate index that we will define in the proof. To further simplify the notation, we let $\rho_i^* \equiv \mathcal{H}_1^*(q_i^*)$ and $\rho_i \equiv \mathcal{H}_1(q_i)$ for all $i \in 1,..,\alpha(\mu_{\vec{\beta}})$. ($q_i$ and q_i^* denote respectively the i^{th} query to $\mathcal{H}_1$ and to $\mathcal{H}_1^*$).

Let's take a closer look at $P_{\omega,r,'\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\mathcal{S}^{\mathcal{H}_T(r')}} succeeds\ in\ EFACM\cap\overline{Col}]$.

Any successful forgery $(I, c_1, r_1, ..., r_n)$ must pass the verification equation $c_1 = \mathcal{H}_1(m, L'_n, R'_n) \pmod l$ where we let $c'_1 \equiv c_1$, and $\forall i \in \{1,..,n\}$:

$\{\ L'_i = (r_i \otimes G) \oplus (c'_i \otimes y_i)$

$\{\ R'_i = (r_i \otimes \mathcal{H}_2(y_i)) \oplus (c'_i \otimes I)$

$\{\ c'_{i+1} = \mathcal{H}_1(m, L'_i, R'_i)$

We distinguish between 3 scenarios (without loss of generality, we assume that all $\mathcal{A}$-queries sent to RO $\mathcal{H}_1$ are distinct from each-other. Similarly, all $\mathcal{A}$-queries sent to

RO $\mathcal{H}_T$ are distinct from each-other. This is because we can assume that $\mathcal{A}$ keeps a local copy of previous query results and avoid redundant calls):

- Scenario 1: $\mathcal{A}$ was successful in its forgery, and
  - No collisions occured, and
  - $\exists i \in \{1, .., n\}$ such that it never queried RO $\mathcal{H}_1$ on input (m, L'_i, R'_i).
- Scenario 2: $\mathcal{A}$ was successful in its forgery, and
  - No collisions occured, and
  - $\forall i \in \{1, .., n\}$ it queried RO $\mathcal{H}_1$ on input (m, L'_i, R'_i) during execution, and
  - $\exists i \in \{1, .., n\}$ such that it queried RO $\mathcal{H}_T$ on input y_i after it had queried RO $\mathcal{H}_1$ on input (m, L'_i, R'_i).
- Scenario 3: $\mathcal{A}$ was successful in its forgery, and
  - No collisions occured, and
  - $\forall i \in \{1, .., n\}$ it queried RO $\mathcal{H}_1$ on input (m, L'_i, R'_i) during execution, and
  - $\forall i \in \{1, .., n\}$, it queried RO $\mathcal{H}_T$ on input y_i before it queried RO $\mathcal{H}_1$ on input $(m, L'_i, , R'_i)$.

The probability of scenario 1 is upper-bounded by the probability that $\mathcal{A}$ picks c'_{i+1} such that it matches the value of $\mathcal{H}_1(m, L'_i, R'_i)$. If the 2 values don't match, then c_1 will be different than c'_{n+1} (by the verification algorithm $\mathcal{V}$). It is upper-bounded because at the very least, this constraint must be observed to pass the verification test. Here, $\mathcal{H}_1(m, L'_i, R'_i)$ is the value that RO $\mathcal{H}_1$ returns to $\mathcal{V}$ (the verification algorithm) when verifying the validity of the forged signature. And since c'_{i+1} can be any value in the range of $\mathcal{H}_1$ (which was defined to be $\mathbb{F}_q$) we get:

$$P[Scenario\ 1] \leq \frac{1}{q} < \frac{1}{l} = \frac{1}{|\{G\}|} < \frac{1}{|\{G\}^*|} \leq \frac{1}{2^k}, \text{ which is negligible in } k.$$

In scenario 2, let $i \in \{1, .., n\}$ be an index such that $\mathcal{A}$ queried RO $\mathcal{H}_T$ on input y_i after it had queried RO $\mathcal{H}_1$ on input (m, L'_i, R'_i). Note that during the verification process, $\mathcal{V}$ will calculate $R'_i \equiv (r_i \otimes \mathcal{H}_2(y_i)) \oplus (c'_i \otimes I)$ and hence will make a call to $\mathcal{H}_T$ on input y_i (*remember that* $\mathcal{H}_2$ *is derived from* $\mathcal{H}_T$). The probability that the resulting R'_i matches the R'_i argument previously fed to $\mathcal{H}_1$ is upper-bounded by $\frac{1}{|\{G\}^*|}$ (since the range of $\mathcal{H}_2 = |\{G\}^*|$). Moreover, i can be any index in $\{1, .., n\}$. We get:

$$P[Scenario\ 2] \leq \frac{n}{|\{G\}^*|} \leq \frac{n}{2^k}, \text{ which is negligible in } k.$$

So we assume that a successful forgery will likely be of the Scenario 3 type.

$$P[Scenario\ 3] = P_{\omega, r, '\mathcal{H}_1, \mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1, \mathcal{H}_T, \mathcal{S}^{\mathcal{H}_T}(r')} succeeds\ in\ EFACM\ \cap \overline{Col}] - P[Scenario\ 1] - P[Scenario\ 2]$$

$$\geq \epsilon(k) - \delta(k) - \frac{1}{2^k} - \frac{n}{2^k} \equiv \nu(k), \text{ which is non-negligible in } k$$

Note that $\mathcal{A}(\omega)$ can send queries to RO $\mathcal{H}_1$ and RO $\mathcal{H}_T$ in any order it chooses to. This gives 2 different ways of referencing the index of a particular query sent to RO $\mathcal{H}_1$. One way is to count the index as it appeared in the sequence of cumulative queries sent to both $\mathcal{H}_1$ and $\mathcal{H}_T$. In this case, indices take on values in $\{1, .., Q_1 + Q_T\}$. The other way, is to do the counting with respect to $\mathcal{H}_1$ queries only causing indices to take on values in $\{1, .., Q_1\}$. If i is the index counted in the cumulative numbering system (i.e., the former system), we let $\alpha(i)$ be the equivalent index in the latter system. Clearly, $\alpha(i) \leq i$.

By definition of scenario 3, we know for a fact that $\forall i \in \{1, ..., n\}$, there exists an integer $l_i \in \{1, ..., Q_1 + Q_T\}$ such that l_i is the index of the query (m, L'_i, R'_i). We define $Ind(\omega, r', \mathcal{H}_1, \mathcal{H}_T)$ to be the vector of indices $(l_1, ..., l_n)$ corresponding to the queries $(m, L'_i, R'_i), i \in \{1, ..., n\}$ that $\mathcal{A}(\omega)$ sends to RO $\mathcal{H}_1$ during execution. Here, indexing is with respect to the cumulative numbering system. We let $l_i = \infty$ if query (m, L'_i, R'_i) was never asked by $\mathcal{A}(\omega)$. We also define the following condition:

$$E \equiv \{\forall i \in \{1, .., n\}, \mathcal{A}(\omega) \textit{ queried RO } \mathcal{H}_T \textit{ on input } y_i \textit{ before it queried RO } \mathcal{H}_1 \textit{ on input } (m, L'_i, R'_i)\}.$$

This definition allows us to build the following sets:

- $S=\{(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \mid \mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\mathcal{S}^{\mathcal{H}_T(r')}} \textit{succeeds in EFACM} \cap \overline{Col} \cap E \cap max_{i=1}^{n}[Ind(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\neq\infty]\}$

  In other terms, S is the set of tuples $(\omega, r', \mathcal{H}_1, \mathcal{H}_T)$ that yield a successful EFACM forgery when no collisions occur, and when $\mathcal{A}(\omega)$ queried RO $\mathcal{H}_1$ on input $(m, L'_i, R'_i), \forall i \in \{1, ..., n\}$ at some point during its execution such that condition E is met. This is none other than scenario 3.

- $S_{\vec{l}} =\{(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \mid \mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\mathcal{S}^{\mathcal{H}_T(r')}} \textit{succeeds in EFACM} \cap \overline{Col} \cap E \cap Ind(\omega,r',\mathcal{H}_1,\mathcal{H}_T)=\vec{l}\}$

  where

  $$\vec{l} \in N_n \equiv \{(l_1, ., l_n) \mid (1 \leq l_i \leq Q_1 + Q_T) \cap (\forall i, j \in \{1, ., n\}, (i \neq j) \Rightarrow (l_i \neq l_j))\}.$$

  We let $V_{(Q_1+Q_T),n}$ denote that the cardinality of L_n. We have

  $$V_{(Q_1+Q_T),n} = (Q_1 + Q_T).(Q_1 + Q_T - 1)...(Q_1 + Q_T - n + 1).$$

  We can see that $S_{\vec{l}}$ represents the set of tuples $(\omega, r', \mathcal{H}_1, \mathcal{H}_T)$ that yield a successful EFACM forgery when no collisions occur, and when $\mathcal{A}(\omega)$ queried RO $\mathcal{H}_1$ on all $(m, L'_i, R'_i), \forall i \in \{1, ..., n\}$ such that the index of the input query (m, L'_i, R'_i) is equal to $(\vec{l})_i$ (i.e., the i^{th} component of $\vec{l}$), and such that condition E is met.

Recall that, $P_{\omega,r',\mathcal{H}_1,\mathcal{H}_T}[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S] = P[Scenario\ 3] \geq \nu(k)$, (non-negligible in k).

Clearly, $\{\cup_{\vec{l}\in N_n} S_{\vec{l}}\}$ partitions S. So $\sum_{\vec{l}\in N_n} P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S] = 1$.

This implies that $\exists \vec{l} \in N_n \textit{ s.t. } P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S] \geq \frac{1}{2V_{(Q_1+Q_T),n}}$.

If this were not the case, then one would get the following contradiction:

$$1 = \sum_{\vec{l} \in N_n} P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S] < V_{(Q_1+Q_T),n} \times \frac{1}{2V_{(Q_1+Q_T),n}} = \frac{1}{2} < 1.$$

So we introduce the set I consisting of all vectors $\vec{l}$ that meet the $\frac{1}{2V_{(Q_1+Q_T),n}}$ threshold, i.e.

$$I = \{\vec{l} \in N_n \; s.t \; P[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S_{\vec{l}} \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S] \geq \frac{1}{2V_{(Q_1+Q_T),n}}\}$$

We claim that $P[Ind(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in I \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S] \geq \frac{1}{2}$.

Proof: By definition of the sets $S_{\vec{l}}$, we have:

$$P[Ind(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in I \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S] = \sum_{\vec{l} \; in \; I} P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S]$$

$$= 1-\sum_{\vec{u}\notin I} P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S_{\vec{u}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T)\in S] > 1-\sum_{\vec{u}\notin I} \frac{1}{2V_{(Q_1+Q_T)}} > 1-\frac{V_{(Q_1+Q_T),n}}{2V_{(Q_1+Q_T),n}} = \frac{1}{2}$$

The next step is to apply the splitting lemma to each $S_{\vec{l}}$, $\vec{l} \in I$. First note that:

$$P_{\omega,r',\mathcal{H}_1,\mathcal{H}_T}[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S_{\vec{l}}] = P_{\omega,r',\mathcal{H}_1,\mathcal{H}_T}[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (S_{\vec{l}} \cap S)]$$

$$= P[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S_{\vec{l}} \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S] \times P_{\omega,r',\mathcal{H}_1,\mathcal{H}_T}[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S]$$

$$\geq \frac{1}{2V_{(Q_1+Q_T),n}} \times \nu(k)$$

Let $\mu_{\vec{l}} \equiv max\{(\vec{l})_1, ..., (\vec{l})_n\}$. Referring to the notation used in the splitting lemma (section 7 of part 1), we let:

- $A \equiv S_{\vec{l}}$
- $X \equiv (\omega, r', \rho_1, ..., \rho_{\alpha(\mu_{\vec{l}})-1}, \mathcal{H}_T)$
- $Y \equiv (\rho_{\alpha(\mu_{\vec{l}})}, ..., \rho_{Q_1})$
- $\epsilon \equiv \frac{\nu(k)}{2V_{(Q_1+Q_T),n}}$
- $\alpha \equiv \frac{\nu(k)}{4V_{(Q_1+Q_T),n}} = \frac{\epsilon}{2}$

X is defined as the space of tuples of:

- All random tapes ω
- All random tapes r'
- All possibe RO $\mathcal{H}_1$ answers to the first $(\alpha(\mu_{\vec{l}}) - 1)$ queries sent by $\mathcal{A}(\omega)$ (note the usage of α-indexing since indexing is done with respect to RO $\mathcal{H}_1$ queries only)

- All RO $\mathcal{H}_T$ (this means all possible RO $\mathcal{H}_T$ answers to the Q_T queries sent by $\mathcal{A}(\omega)$).

Y is defined as the space of all possible RO $\mathcal{H}_1$ answers to the last $(Q_1 - \alpha(\mu_{\vec{l}}) + 1)$ queries sent by $\mathcal{A}(\omega)$. (Recall that $\rho_j \equiv \mathcal{H}_1(q_j)$ where q_j is the j^{th} query sent to RO $\mathcal{H}_1$).

The splitting lemma guarantees the existence of a subset $\Omega_{\vec{l}}$ of tuples $(\omega, r', \mathcal{H}_1, \mathcal{H}_T)$ such that:

- $P_{\omega,r',\mathcal{H}_1,\mathcal{H}_T}[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in \Omega_{\vec{l}}] \geq \frac{\nu(k)}{4V_{(Q_1+Q_T),n}}$
- $\forall[(\omega^{\sim}, r'^{\sim}, \mathcal{H}_1^{\sim}, \mathcal{H}_T^{\sim}) \equiv (\omega^{\sim}, r'^{\sim}, \rho_1^{\sim}, ., \rho_{\alpha(\mu_{\vec{l}})-1}^{\sim},\ \rho_{\alpha(\mu_{\vec{l}})}^{\sim}, ., \rho_{Q_1}^{\sim}, \mathcal{H}_T^{\sim})] \in \Omega_{\vec{l}}$, we have

$$P_{\mathcal{H}_1}[(\omega^{\sim}, r'^{\sim},\ \rho_1^{\sim}, .., \rho_{\alpha(\mu_{\vec{l}})-1}^{\sim},\ \rho_{\alpha(\mu_{\vec{l}})}, .., \rho_{Q_1}, \mathcal{H}_T^{\sim}) \in S_{\vec{l}} \mid (\omega^{\sim}, r'^{\sim}, \mathcal{H}_1^{\sim}, \mathcal{H}_T^{\sim}) \in \Omega_{\vec{l}}] \geq \frac{\nu(k)}{4V_{(Q_1+Q_T),n}}, \text{ and so}$$

$$P_{\mathcal{H}_1}[(\omega^{\sim}, r'^{\sim}, \mathcal{H}_1, \mathcal{H}_T^{\sim}) \in S_{\vec{l}} \mid (\omega^{\sim}, r'^{\sim}, \mathcal{H}_1^{\sim}, \mathcal{H}_T^{\sim}) \in \Omega_{\vec{l}},\ \rho_1 = \rho_1^{\sim}\ ,...,\ \rho_{\alpha(\mu_{\vec{l}})-1} = \rho_{\alpha(\mu_{\vec{l}})-1}^{\sim})] \geq \frac{\nu(k)}{4V_{(Q_1+Q_T),n}}$$

- $P[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in \Omega_{\vec{l}} \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S_{\vec{l}}] \ \geq\ (\frac{\nu(k)}{4V_{(Q_1,+Q_T),n}})/(\frac{\nu(k)}{2V_{(Q_1+Q_T),n}}) \ =\ \frac{1}{2}$

We would like to compute the probability of finding a 2^{nd} successful tuple $(\omega^*, r'^*, \mathcal{H}_1^{\sim}, \mathcal{H}_T^*)$ given that $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$ was a successful 1^{st} tuple and such that $\rho_j^{\sim} = \rho_j^*,\ \forall j \in \{1, .., \alpha(\mu_{\vec{l}}) - 1\}$. That means finding the following probability:

$$P_{\mathcal{H}_1}[(\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{l}} \mid (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in S_{\vec{l}},\ \rho_1 = \rho_1^*, ..., \rho_{\alpha(\mu_{\vec{l}})-1} = \rho_{\alpha(\mu_{\vec{l}})-1}^*].$$

From the splitting lemma results, we have a (non-negligible in k) lower-bound on $P_{\mathcal{H}_1}[(\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{l}} \mid (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in \Omega_{\vec{l}},\ \rho_1 = \rho_1^*, ..., \rho_{\alpha(\mu_{\vec{l}})-1} = \rho_{\alpha(\mu_{\vec{l}})-1}^*]$.

Note however, that $\Omega_{\vec{l}}$ and $S_{\vec{l}}$ are generally distinct sets. And so we **cannot** conclude that

$$P_{\mathcal{H}_1}[(\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{l}} \mid (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in S_{\vec{l}},\ \rho_1 = \rho_1^*, ..., \rho_{\alpha(\mu_{\vec{l}})-1} = \rho_{\alpha(\mu_{\vec{l}})-1}^*]$$

$$= P_{\mathcal{H}_1}[(\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{l}} \mid (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in \Omega_{\vec{l}},\ \rho_1 = \rho_1^*, ..., \rho_{\alpha(\mu_{\vec{l}})-1} = \rho_{\alpha(\mu_{\vec{l}})-1}^*]$$

and therefore we **cannot** conclude that the following quantity is non-negligible in k

$$P_{\mathcal{H}_1}[(\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{l}} \mid (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in S_{\vec{l}},\ \rho_1 = \rho_1^*, ..., \rho_{\alpha(\mu_{\vec{l}})-1} = \rho_{\alpha(\mu_{\vec{l}})-1}^*]$$

In order to show that the above quantity is non-negligible in k, we proceed differently. Suppose we can show that the following probability is non-negligible in k:

$$P_{(\omega,r',\mathcal{H}_1,\mathcal{H}_T)}[\exists \vec{\beta} \in I \ s.t.\ (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}})]$$

This would imply that with non-negligible probability, we can find a tuple that belongs to $S_{\vec{\beta}}$ (and hence corresponds to a successful forgery) and at the same time belongs to

$\Omega_{\vec{\beta}}$. We can then invoke the splitting lemma result just mentioned, to find a second tuple coresponding to a second forgery and that has the desired properties.

To prove the above, we proceed as follows:

$$P[\exists \vec{\beta} \in I \ s.t. \ (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}}) \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S]$$

$$= P[\cup_{\vec{l} \in I} \{(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (\Omega_{\vec{l}} \cap S_{\vec{l}}) \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S\}]$$

$= \sum_{\vec{l} \in I} P[(\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (\Omega_{\vec{l}} \cap S_{\vec{l}}) \mid (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in S]$, since the $S_{\vec{l}}$'s are disjoint.

$= \sum_{\vec{l} \in I} \{ \ P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in \Omega_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in (S_{\vec{l}} \cap S)] \ \times \ P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S] \ \}$

$= \sum_{\vec{l} \in I} \{ \ P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in \Omega_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S_{\vec{l}}] \ \times \ P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S] \ \}$

$\geq \frac{1}{2} \sum_{\vec{l} \in I} P[(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S_{\vec{l}} \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S]$, *($3^{rd}$ result of splitting lemma above)*

$\geq \frac{1}{2} \times \frac{1}{2}$ *(by the claim proven earlier)* $= \frac{1}{4}$.

And so we conclude that:

$$P_{(\omega,r',\mathcal{H}_1,\mathcal{H}_T)}[\exists \vec{\beta} \in I \ s.t. \ (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}})]$$

$$= P_{(\omega,r',\mathcal{H}_1,\mathcal{H}_T)}[\exists \vec{\beta} \in I \ s.t. \ (\omega, r', \mathcal{H}_1, \mathcal{H}_T) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}} \cap S)]$$

$= P[\exists \vec{\beta} \in I \ s.t. \ (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}}) \mid (\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S] \ \times \ P_{(\omega,r',\mathcal{H}_1,\mathcal{H}_T)}[(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \in S] \geq \frac{\nu(k)}{4}$

which is non-negligible in k.

So let $\vec{\beta}$ be such an index and $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$ such a tuple. From the result above, we know that finding such a $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}})$ can be done with non-negligible probability. And since $(\Omega_{\vec{\beta}} \cap S_{\vec{\beta}}) \subset \Omega_{\vec{\beta}}$, we must have $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in \Omega_{\vec{\beta}}$. We can then invoke the 2^{nd} consequence of the splitting lemma and write:

$$P_{\mathcal{H}_1}[(\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{\beta}} \mid (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in S_{\vec{\beta}}, \ \rho_1 = \rho_1^*, .., \rho_{\alpha(\mu_{\vec{\beta}})-1} = \rho^*_{\alpha(\mu_{\vec{\beta}})-1})] =$$

$$P_{\mathcal{H}_1}[(\omega^*,r'^*,\mathcal{H}_1,\mathcal{H}_T^*) \in S_{\vec{\beta}} \mid (\omega^*,r'^*,\mathcal{H}_1^*,\mathcal{H}_T^*) \in \Omega_{\vec{\beta}}, \ \rho_1 = \rho_1^*,..,\rho_{\alpha(\mu_{\vec{\beta}})-1} = \rho^*_{\alpha(\mu_{\vec{\beta}})-1})] \geq \frac{\nu(k)}{4V_{(Q_1+Q_T),n}}$$

We still have one last constraint to impose and that is that $\rho^*_{\alpha(\mu_{\vec{\beta}})} \neq \rho_{\alpha(\mu_{\vec{\beta}})}$. We show that the following quantity is non-negligible:

$$P_{\mathcal{H}_1}[((\omega^*, r'^*, \mathcal{H}_1, \mathcal{H}_T^*) \in S_{\vec{\beta}}) \ \cap \ (\rho_{\alpha(\mu_{\vec{\beta}})} \neq \rho^*_{\alpha(\mu_{\vec{\beta}})}) | \ (\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in S_{\vec{\beta}}, \ \rho_1 = \rho_1^*, ..., \rho_{\alpha(\mu_{\vec{\beta}})-1} = \rho^*_{\alpha(\mu_{\vec{\beta}})-1})]$$

To prove this, we use the same technique employed in part 2 and part 4 of this series. Note that if B and C are independent events, then we can write:

$$P[A|C] = P[A \cap B|C] + P[A \cap \overline{B}|C] \leq P[A \cap B|C] + P[\overline{B}|C] = P[A \cap B|C] + P[\overline{B}]$$

And so we get $P[A \cap B|C] \geq P[A|C] - P[\overline{B}]$.

This result allows us to write:

$$P_{\mathcal{H}_1}[((\omega^*,r'^*,\mathcal{H}_1,\mathcal{H}_T^*) \in S_{\vec{\beta}}) \cap (\rho_{\alpha(\mu_{\vec{\beta}})} \neq \rho^*_{\alpha(\mu_{\vec{\beta}})}) \mid (\omega^*,r'^*,\mathcal{H}_1^*,\mathcal{H}_T^*) \in S_{\vec{\beta}},\ \rho_1=\rho_1^* \ldots,\ \rho_{\alpha(\mu_{\vec{\beta}})-1}=\rho^*_{\alpha(\mu_{\vec{\beta}})-1})]$$

$$\geq P_{\mathcal{H}_1}[(\omega^*,r'^*,\mathcal{H}_1,\mathcal{H}_T^*) \in S_{\vec{\beta}} \mid (\omega^*,r'^*,\mathcal{H}_1^*,\mathcal{H}_T^*) \in S_{\vec{\beta}},\ \rho_1=\rho_1^*\ ,\ldots,\ \rho_{\alpha(\mu_{\vec{\beta}})-1}=\rho^*_{\alpha(\mu_{\vec{\beta}})-1})] - P_{\mathcal{H}_1}[\rho_{\alpha(\mu_{\vec{\beta}})} = \rho^*_{\alpha(\mu_{\vec{\beta}})}]$$

$$= P_{\mathcal{H}_1}[(\omega^*,r'^*,\mathcal{H}_1,\mathcal{H}_T^*) \in S_{\vec{\beta}} \mid (\omega^*,r'^*,\mathcal{H}_1^*,\mathcal{H}_T^*) \in \Omega_{\vec{\beta}},\ \rho_1=\rho_1^*\ ,\ldots,\ \rho_{\alpha(\mu_{\vec{\beta}})-1}=\rho^*_{\alpha(\mu_{\vec{\beta}})-1})] - P_{\mathcal{H}_1}[\rho_{\alpha(\mu_{\vec{\beta}})} = \rho^*_{\alpha(\mu_{\vec{\beta}})}]$$

(because we chose $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in \Omega_{\vec{\beta}} \cap S_{\vec{\beta}}$*)*

$$\geq \frac{\nu(k)}{4V_{(Q_1+Q_T),n}} - \frac{1}{2^k}, \text{ which is non-negligible in } k.$$

Step 5 : The final step uses the 2 forgeries obtained earlier to solve an instance of the Discrete Logarithm (DL) problem. Here is a recap of Step 4 results:

- With non-negligible probability of at least $\frac{\nu(k)}{4}$ we get a successful tuple $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$, s.t. $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}})$ for some vector of indices $\vec{\beta} \in I$. By running $\mathcal{A}$ a number of times polynomial in k, we can find such a tuple.
- Once we find such a tuple, we've also shown that with non-negligible probability of at least $\frac{\nu(k)}{4V_{(Q_1+Q_T),n}} - \frac{1}{2^k}$, we can find another successful tuple $(\omega^*, r'^*, \mathcal{H}_1^{\sim}, \mathcal{H}_T^*)$ s.t. $(\omega^*, r'^*, \mathcal{H}_1^{\sim}, \mathcal{H}_T^*) \in S_{\vec{\beta}}$ and $(\rho_1^{\sim} = \rho_1^*), .., (\rho^{\sim}_{\alpha(\mu_{\vec{\beta}})-1} = \rho^*_{\alpha(\mu_{\vec{\beta}})-1}),\ (\rho^{\sim}_{\alpha(\mu_{\vec{\beta}})} \neq \rho^*_{\alpha(\mu_{\vec{\beta}})})$.

Let $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$ correspond to forgery $\sigma_a(m_a, L) \equiv (I_a, (c_1)_a, (r_1)_a, .., (r_n)_a)$, and $(\omega^*, r'^*, \mathcal{H}^{\sim}, \mathcal{H}_T^*)$ correspond to forgery $\sigma_b(m_b, L) \equiv (I_b, (c_1)_b, (r_1)_b, .., (r_n)_b)$.

Recall that $\alpha(\mu_{\vec{\beta}})$ is the index of the last query of the form $(m, L'_i, R'_i),\ i \in \{1, ..., n\}$ that $\mathcal{A}$ sends to RO $\mathcal{H}_1$ ($\mu_{\vec{\beta}} = max_{i=1}^n(\vec{\beta})_i$). Since the 2 experiments corresponding to the 2 successful tuples have:

- The same random tapes ω^* and r'^*
- The same RO $\mathcal{H}_T^*$
- ROs $\mathcal{H}_1^*$ and $\mathcal{H}_1^{\sim}$ behave the same way on the first $\alpha(\mu_{\vec{\beta}}) - 1$ queries,

we can be confident that the first $\alpha(\mu_{\vec{\beta}})$ queries sent to the 2 ROs $\mathcal{H}_1^*$ and $\mathcal{H}_1^{\sim}$ are identical. In other words, we have $(m_a, (L'_i)_a, (R'_i)_a) = (m_b, (L'_i)_b, (R'_i)_b), \forall i \in \{1, ..., n\}$. Without loss of generality, let (m, L'_ζ, R'_ζ), (where $\zeta \in \{1, ..., n\}$), correspond to the last query of this type sent to RO $\mathcal{H}_1$. That means that (m, L'_ζ, R'_ζ) is the $\mu_{\vec{\beta}}^{th}$ query sent to RO $\mathcal{H}_1$. We have:

$$(m_a, (L'_{\zeta+1})_a, (R'_{\zeta+1})_a) = (m_b, (L'_{\zeta+1})_b, (R'_{\zeta+1})_b) \text{ (where } (\zeta+1) \equiv 1 \text{ whenever } \zeta = n)$$

$$\implies (L'_{\zeta+1})_a = (L'_{\zeta+1})_b$$

$$\implies ((r_{\zeta+1})_a \otimes G) \oplus ((c'_{\zeta+1})_a \otimes y_{\zeta+1}) = ((r_{\zeta+1})_b \otimes G) \oplus ((c'_{\zeta+1})_b \otimes y_{\zeta+1}),$$

$$\implies x_{\zeta+1}[(c'_{\zeta+1})_a - (c'_{\zeta+1})_b] = (r_{\zeta+1})_b - (r_{\zeta+1})_a \pmod{l} \text{ (by writing } y_{\zeta+1} = x_{\zeta+1} \otimes G)$$

Moreover, we have

$$(c'_{\zeta+1})_a = \mathcal{H}_1^*(m_a, (L'_\zeta)_a, (R'_\zeta)_a) \pmod{l} \textit{ (by definition of } c' \textit{ in } \mathcal{V})$$

$$= \rho^*_{\alpha(\mu_{\vec{\beta}})} \neq \rho^{\sim}_{\alpha(\mu_{\vec{\beta}})} \textit{ (by design of the forgery tuples)}$$

$$= \mathcal{H}_1^{\sim}(m_b, (L'_\zeta)_b, (R'_\zeta)_b) \pmod{l} = (c'_{\zeta+1})_b \textit{ (by definition of } c' \textit{ in } \mathcal{V})$$

That means that we can solve for $x_{\zeta+1} = \frac{(r_{\zeta+1})_b - (r_{\zeta+1})_a}{(c'_{\zeta+1})_a - (c'_{\zeta+1})_b} \pmod{l}$ in polynomial time, contradicting the intractability of DL on elliptic curve groups. We conclude that the signature scheme is secure against EFACM in the RO model.

5 Security analysis - Exculpability

In part 5 of this series we discussed 2 different notions of *exculpability*. One of them had to do with the security property of *anonymity* and the other with the security property of *unforgeability*. Exculpability in the anonymity sense roughly meant that a signer's identity can not be established even if her private key gets compromised (i.e., no one can prove that she was the actual signer under any circumstance). This section is concerned with the notion of exculpability from an unforgeability standpoint as described in [2].

The setting is similar to the one previously described in part 5. Suppose $(n-1)$ private keys have been compromised in an n-ring setting. Let π denote the index of the only non-compromised private key x_π, and let I_π denote the key-image (or tag) associated with the key pair (x_π, y_π). We investigate whether it is likely to produce a valid forgery with key-image I_π. In what follows, we show that this can only happen with negligible probability. In essence, this means that a non-compromised honest ring member (*by honest we mean a ring member that signs at most once using his private key*) does not run the risk of encountering a forged signature that carries his key-image. In the context of Cryptonote, this implies that a non-compromised honest ring member cannot be accused of signing twice using the same key image or tag, and hence is exculpable.

Note that since the adversary $\mathcal{A}(\omega)$ has access to the $(n-1)$ compromised private keys, it can easily calculate their corresponding public keys. Doing so will allow it to identify the public key y_π of the non-compromised ring member. That means that it can determine the index π of the non-compromised member in the ring $L \equiv \{y_1, .., y_n\}$. In order to prove the exculpability of LSAG, we follow an almost identical proof to that of the previous section (i.e., unforgeability vis-a-vis EFACM) and apply the same 5-step approach. The objective is to show that this particular type of forgery would imply the

ability to solve the DL of y_π. The nuance resides in the specific index π for which the DL will be solved, as opposed to any other index. This is because we assume that all the other members are compromised and hence their DLs (i.e., private keys) are common-knowledge.

Step 1 : We proceed by contradiction and assume that there exists a PPT adversary $\mathcal{A}$ such that:

$$P_{\omega,r,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\{x_1,..,\hat{x_\pi},..,x_n\},\Sigma^{\mathcal{H}_1,\mathcal{H}_T}(r)} \textit{ succeeds in creating a forgery } \sigma(m,L) \equiv (I_\pi, c_1, r_1, ..r_n)] = \epsilon(k), \text{ for } \epsilon \text{ non-negligible in } k.$$

We refer to the event *succeeds in creating a forgery* $\sigma(m,L) \equiv (I_\pi, c_1, r_1, ..r_n)$ as *succeeds in* $EFACM_{Ex_\pi}$. We re-write the above equation as:

$$P_{\omega,r,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\{x_1,..,\hat{x_\pi},..,x_n\},\Sigma^{\mathcal{H}_1,\mathcal{H}_T}(r)} \textit{ succeeds in } EFACM_{Ex_\pi}] = \epsilon(k), \text{ for } \epsilon \text{ non-negligible in } k.$$

The notation used makes it explicit that $\mathcal{A}(\omega)$ can access the set of compromised keys $\{x_1, .., \hat{x_\pi}, .., x_n\}$ with x_π excluded. Success is defined as issuing a forged signature with key image or tag equal to $I_\pi \equiv x_\pi \otimes \mathcal{H}_2(y_\pi)$. (*Recall that* $\mathcal{H}_2$ *is derived from* $\mathcal{H}_T$).

Step 2 : The next step consists in building a simulator $\mathcal{S}(r')$ such that it:

- Does not have access to the private key of any signer.
- Has the same range as the original signing algorithm Σ (i.e., they output signatures taken from the same pool of potential signatures over all possible choices of RO functions and respective random tapes r' and r).
- Has indistinguishable probability distribution from that of Σ over this range.

The simulator $S(r')$ is the same as the one we built in the previous section. The only nuance is that $S(r')$ does not choose a random index π, since $\mathcal{A}(\omega)$ already knows the index of the non-compromised ring member.

Step 3 : The logical reasoning and procedure are identical to those of the previous section. We conclude that

$$P_{\omega,r,'\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\{x_1,..,\hat{x_\pi},..,x_n\},\mathcal{S}^{\mathcal{H}_T(r')}} \textit{succeeds in } EFACM_{Ex_\pi} \cap \overline{Col}] \geq \epsilon(k) - \delta(k).$$

Step 4 : Here too, the logical reasoning and procedure are identical to those of the previous section. In particular, we define the following sets in a similar way:

- $S=$ $\{(\omega,r',\mathcal{H}_1,\mathcal{H}_T)|\ \mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\{x_1,..,\hat{x_\pi},..,x_n\}},\ \mathcal{S}^{\mathcal{H}_T(r')} \textit{succeeds in } EFACM_{Ex_{x_\pi}} \cap \overline{Col} \cap E \cap \max_{i=1}^{n}[Ind(\omega,r',\mathcal{H}_1,\mathcal{H}_T) \neq \infty]\}$

- $S_{\vec{l}}$= $\{(\omega,r',\mathcal{H}_1,\mathcal{H}_T)|\ \mathcal{A}(\omega)^{\mathcal{H}_1,\mathcal{H}_T,\{x_1,..,\hat{x_\pi},..,x_n\}},\ \mathcal{S}^{\mathcal{H}_T(r')} succeeds\ in\ EFACM_{Ex_{x_\pi}} \cap\ \overline{Col} \cap E \cap\ Ind(\omega,r',\mathcal{H}_1,\mathcal{H}_T)=\vec{l}\}$

and conclude that:

$$P_{\mathcal{H}_1}[((\omega^*,r'^*,\mathcal{H}_1,\mathcal{H}_T^*) \in S_{\vec{\beta}}) \cap (\rho_{\alpha(\mu_{\vec{\beta}})} \neq \rho^*_{\alpha(\mu_{\vec{\beta}})}) \mid (\omega^*,r'^*,\mathcal{H}_1^*,\mathcal{H}_T^*) \in S_{\vec{\beta}},\ \rho_1=\rho_1^*\ ...,\ \rho_{\alpha(\mu_{\vec{\beta}})-1}=\rho^*_{\alpha(\mu_{\vec{\beta}})-1})]$$

$$\geq \frac{\nu(k)}{4V_{(Q_1+Q_T),n}} - \frac{1}{2^k}, \text{ which is non-negligible in } k.$$

Here $\alpha(\mu_{\vec{\beta}})$, as before, is an appropriately defined index, $\rho_i^* \equiv \mathcal{H}_1^*(q_i)$, and $\rho_i \equiv \mathcal{H}_1(q_i)$ for all $i \in 1,..,\alpha(\mu_{\vec{\beta}})$.($q_i$ denotes the i^{th} query sent to RO).

Step 5 : The final step uses the 2 forgeries obtained earlier to solve an instance of the Discrete Logarithm (DL) problem. Here is a recap of Step 4 results:

- With non-negligible probability of at least $\frac{\nu(k)}{4}$ we get a successful tuple $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$, s.t. $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*) \in (\Omega_{\vec{\beta}} \cap S_{\vec{\beta}})$ for some vector of indices $\vec{\beta} \in I$. By running $\mathcal{A}$ a number of times polynomial in k, we can find such a tuple.
- Once we find such a tuple, we've also shown that with non-negligible probability of at least $\frac{\nu(k)}{4V_{(Q_1+Q_T),n}} - \frac{1}{2^k}$, we can find another successful tuple $(\omega^*, r'^*, \mathcal{H}_1^\sim, \mathcal{H}_T^*)$ s.t. $(\omega^*, r'^*, \mathcal{H}_1^\sim, \mathcal{H}_T^*) \in S_{\vec{\beta}}$ and $(\rho_1^\sim = \rho_1^*), .., (\rho^\sim_{\alpha(\mu_{\vec{\beta}})-1} = \rho^*_{\alpha(\mu_{\vec{\beta}})-1}),\ (\rho^\sim_{\alpha(\mu_{\vec{\beta}})} \neq \rho^*_{\alpha(\mu_{\vec{\beta}})})$.

Let $(\omega^*, r'^*, \mathcal{H}_1^*, \mathcal{H}_T^*)$ correspond to forgery $\sigma_a(m_a, L) \equiv (I_\pi, (c_1)_a, (r_1)_a, .., (r_n)_a)$, and $(\omega^*, r'^*, \mathcal{H}^\sim, \mathcal{H}_T^*)$ correspond to forgery $\sigma_b(m_b, L) \equiv (I_\pi, (c_1)_b, (r_1)_b, .., (r_n)_b)$.

Recall that $\alpha(\mu_{\vec{\beta}})$ is the index of the last query of the form (m, L_i', R_i'), $i \in \{1, ..., n\}$ that $\mathcal{A}$ sends to RO $\mathcal{H}_1$ ($\mu_{\vec{\beta}} = max_{i=1}^n(\vec{\beta})_i$). Since the 2 experiments corresponding to the 2 successful tuples have:

- The same random tapes ω^* and r'^*
- The same RO $\mathcal{H}_T^*$
- ROs $\mathcal{H}_1^*$ and $\mathcal{H}_1^\sim$ behave the same way on the first $\alpha(\mu_{\vec{\beta}}) - 1$ queries,

we can be confident that the first $\alpha(\mu_{\vec{\beta}})$ queries sent to the 2 ROs $\mathcal{H}_1^*$ and $\mathcal{H}_1^\sim$ are identical. In other words, we have $(m_a, (L_i')_a, (R_i')_a) = (m_b, (L_i')_b, (R_i')_b), \forall i \in \{1, ..., n\}$.

$\implies \forall i \in \{1, .., n\},\ (L_i')_a = (L_i')_b$, and $(R_i')_a = (R_i')_b$

Let $R_i' \equiv (R_i')_a = (R_i')_b$, and $L_i' \equiv (L_i')_a = (L_i')_b$. For each $i \in \{1, .., n\}$, we get 2 identical systems of 2 equations dictated by $\mathcal{V}$'s verification computation:

First system of 2 linear equations

$$\{\ R_i' = ((r_i)_a \otimes \mathcal{H}_2(y_i)) \oplus ((c_i')_a \otimes I_\pi)$$

$$\{\ L_i' = ((r_i)_a \otimes G) \oplus ((c_i')_a \otimes y_i)$$

where $(c_1')_a \equiv (c_1)_a$, and $(c_{i+1}')_a = \mathcal{H}_1(m_a, (L_i')_a, (R_i')_a)\ \forall i \in \{1, ..., n\}$

Second system of 2 linear equations

$$\{\ L'_i = ((r_i)_b \otimes G) \oplus ((c'_i)_b \otimes y_i)$$

$$\{\ R'_i = ((r_i)_b \otimes \mathcal{H}_2(y_i)) \oplus ((c'_i)_b \otimes I_\pi)$$

where $(c'_1)_b \equiv (c_1)_b$, and $(c'_{i+1})_b = \mathcal{H}_1(m_b, (L'_i)_a, (R'_i)_b)\ \forall i \in \{1, ..., n\}$

$\forall i \in \{1, .., n\}$, the first system is a linear system of 2 equations in variables $(r_i)_a$ and $(c'_i)_a$. Similarly, the second system is a linear system of 2 equations in variables $(r_i)_b$ and $(c'_i)_b$. The 2 systems are identical with different variable names. Hence, if $((r_i)^*_a, (c'_i)^*_a)$ is a unique solution to the first system and $((r_i)^*_b, (c'_i)^*_b)$ a unique solution to the second, we can be confident that $((r_i)^*_a = (r_i)^*_b$ and $(c'_i)^*_a = (c'_i)^*_b$. (Note that when we previously proved resilience against EFACM in section 4, the 2 forged signatures did not necessarily share the same tag I_π and so the 2 systems of linear equations would have been different from each other). For either system to admit a unique solution, the 2 equations must be linearly independent. We re-write the 2 systems as follows:

First system of 2 linear equations

$$\{\ R'_i = ((r_i)_a \otimes \mathcal{H}_2(y_i)) \oplus ((c'_i)_a \otimes I_\pi)$$

$$\{\ log_G(L'_i) = (r_i)_a\ +\ (c'_i)_a\ x_i$$

where $(c'_1)_a \equiv (c_1)_a$, and $(c'_{i+1})_a = \mathcal{H}_1(m_a, (L'_i)_a, (R'_i)_a)\ \forall i \in \{1, ..., n\}$

Second system of 2 linear equations

$$\{\ R'_i = ((r_i)_b \otimes \mathcal{H}_2(y_i)) \oplus ((c'_i)_b \otimes I_\pi)$$

$$\{\ log_G(L'_i) = (r_i)_b\ +\ (c'_i)_b\ x_i$$

where $(c'_1)_b \equiv (c_1)_b$, and $(c'_{i+1})_b = \mathcal{H}_1(m_b, (L'_i)_a, (R'_i)_b)\ \forall i \in \{1, ..., n\}$

If we multiply the second equation by $\mathcal{H}_2(y_i)$ (multiplication refers to $\otimes$), we see that a sufficient condition for the system to be linearly independent is to have $[x_i \otimes \mathcal{H}_2(y_i)]\ \neq\ I_\pi \equiv [x_\pi \otimes \mathcal{H}_2(y_\pi)]$. Next, we show that with overwhelming probability, the system of linear equations is indeed independent for all $i \in \{1, .., n\},\ i \neq \pi$:

- Recall that the range of $\mathcal{H}_2$ is $\{G\}^*$ and that the order of $\{G\}^* = (l-1)$.
- Therefore, $\exists\ v_i,\ v_\pi\ \in \mathbb{F}^*_l$ such that $\mathcal{H}_2(y_i) = v_i \otimes G$ and $\mathcal{H}_2(y_\pi) = v_\pi \otimes G$.
- We can then re-write the sufficient condition as $x_i v_i \neq x_\pi v_\pi\ \pmod l$.
- Note that given x_i, x_π, and v_π, there is at most one value of $v_i \in \mathbb{F}^*_l$ that satisfies $x_i v_i = x_\pi v_\pi\ \pmod l$. Otherwise, we would have $v_i, v'_i \in \mathbb{F}^*_l$, $v_i \neq v'_i\ \pmod l$, and $x_i v_i = x_\pi v_\pi = x_i v'_i$. This would imply that $v_i \equiv v'_i\ \pmod l$, a contradiction.
- Noting that each v_i corresponds to a distinct $\mathcal{H}_2(y_i)$, we conclude that given x_i, x_π and $\mathcal{H}_2(y_\pi)$ there is at most one $\mathcal{H}_2(y_i)$ s.t. $[x_i \otimes \mathcal{H}_2(y_i)]\ =\ I_\pi \equiv [x_\pi \otimes \mathcal{H}_2(y_\pi)]$.
- Since $\mathcal{H}_2$ is a RO outputing random values, the probability of getting the right value of $\mathcal{H}_2(y_i)$ is $\leq \frac{1}{|\{G\}^*|} < \frac{1}{|\{G\}|} < \frac{1}{2^k}$ (negligible in k).

$\forall i \in \{1, .., n\},\ i \neq \pi$, we therefore conclude that with overwhelming probability we have $[x_i \otimes \mathcal{H}_2(y_i)] \neq I_\pi$. We can then be confident that the linear system of 2 equations has a unique solution. Hence, $\forall i \in \{1, .., n\},\ i \neq \pi$, we have $(r_i)_a = (r_i)_b$, and $(c'_i)_a = (c'_i)_b$.

Moreover, by design of the 2 forgeries, we know that there exists one and only one $\zeta \in \{1, ..., n\}$ (corresponding to the $\mu^{th}_{\vec{\beta}}$ query sent to RO $\mathcal{H}_1$) that satisfies

$$(c'_{\zeta+1})_a = \mathcal{H}_1^*(m_a, (L'_\zeta)_a, (R'_\zeta)_a) \pmod{l} \textit{ (by definition of } c' \textit{ in } \mathcal{V})$$

$$= \rho^*_{\alpha(\mu_{\vec{\beta}})} \neq \rho^{\sim}_{\alpha(\mu_{\vec{\beta}})} \textit{ (by design of the forgery tuples)}$$

$$= \mathcal{H}_1^{\sim}(m_b, (L'_\zeta)_b, (R'_\zeta)_b) \pmod{l} = (c'_{\zeta+1})_b \textit{ (by definition of } c' \textit{ in } \mathcal{V})$$

$$(\text{where } (\zeta+1) \equiv 1 \text{ whenever } \zeta = n)$$

But $\forall i \in \{1, .., n\},\ i \neq \pi$, we showed that with overwhelming probability $(c'_i)_a = (c'_i)_b$. Therefore, it must be that $(\zeta + 1) = \pi$ and so $(c'_\pi)_a \neq (c'_\pi)_b$.

Going back to the system of 2 equations associated with $i = \pi$, we write:

$$(r_\pi)_a + (c'_\pi)_a\ x_\pi = log_G(L'_\pi) = (r_\pi)_b + (c'_\pi)_b\ x_\pi$$

That means that we can solve for $x_\pi = \frac{(r_\pi)_b - (r_\pi)_a}{(c'_\pi)_a - (c'_\pi)_b} \pmod{l}$ in polynomial time, contradicting the intractability of DL on elliptic curve groups. We conclude that the signature scheme is exculpable and secure against $EFACM_{Ex_\pi}$ in the RO model.

6 Security analysis - Anonymity

In this section, we show that the LSAG scheme satisfies the weaker anonymity definition #2 introduced in part 3 of this series. Note that as we previously observed in part 5, linkable signatures cannot satisfy anonymity definition #1.

More formally, let $\mathcal{A}(\omega)$ be a PPT adversary with random tape ω that takes 4 inputs:

- Any message m.
- A ring $L \equiv \{y_1, ...y_n\}$ that includes the public key y_π of the actual signer.
- A list $\mathcal{D}_t \equiv \{\hat{x}_1, ...\hat{x}_t\}$ of compromised private keys of ring members ($0 \leq t \leq n$). $\mathcal{D}_t$ can be empty, and $\hat{x}_i$ may be different than x_i, but $\mathcal{D}_t \subseteq \{x_1, ..., x_n\}$
- A valid signature $\sigma_\pi(m, L)$ on message m, ring L and actual signer private key x_π.

$\mathcal{A}(\omega)$ outputs an index in L that it thinks is the actual signer. Definition # 2 mandates that for any polynomial in security parameter k $Q(k)$, we have:

$$\tfrac{1}{n-t} - \tfrac{1}{Q(k)} \leq P[\mathcal{A}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L) \textit{ is valid}] \leq \tfrac{1}{n-t} + \tfrac{1}{Q(k)}$$
$$\text{if } x_\pi \notin \mathcal{D}_t \text{ and } 0 \leq t < n-1.$$

$$P[\mathcal{A}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L) \textit{ is valid}] > 1 - \tfrac{1}{Q(k)}$$
$$\text{if } x_\pi \in \mathcal{D}_t \text{ or } t = n-1.$$

In the RO model, $\mathcal{A}(\omega)$ can send a number of queries (polynomial in k) to RO $\mathcal{H}_1$ and RO $\mathcal{H}_T$. The probability of $\mathcal{A}$'s success is computed over the distributions of $\omega, \mathcal{H}_1$ and $\mathcal{H}_T$. Making explicit the dependence on the ROs, definition # 2's condition becomes:

$$\frac{1}{n-t} - \frac{1}{Q(k)} \leq P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L) \; is \; valid] \leq \frac{1}{n-t} + \frac{1}{Q(k)}$$
$$\text{if } x_\pi \notin \mathcal{D}_t \text{ and } 0 \leq t < n-1.$$

$$P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L) \; is \; valid] > 1 - \frac{1}{Q(k)}$$
$$\text{if } x_\pi \in \mathcal{D}_t \text{ or } t = n-1.$$

In order to prove that anonymity holds in the above sense, we proceed by contradiction and rely on the intractability of the *Decisional Diffie Hellman* problem (*DDH* for short). (Refer to part 5 for a discussion of DDH). We consider 3 separate cases:

- Case 1: $x_\pi \notin \mathcal{D}_t$ and $0 \leq t < n-1$.

  Suppose that $\exists\ \mathcal{A}(\omega)$ in PPT(k) and $\epsilon(k)$ non-negligible in k such that

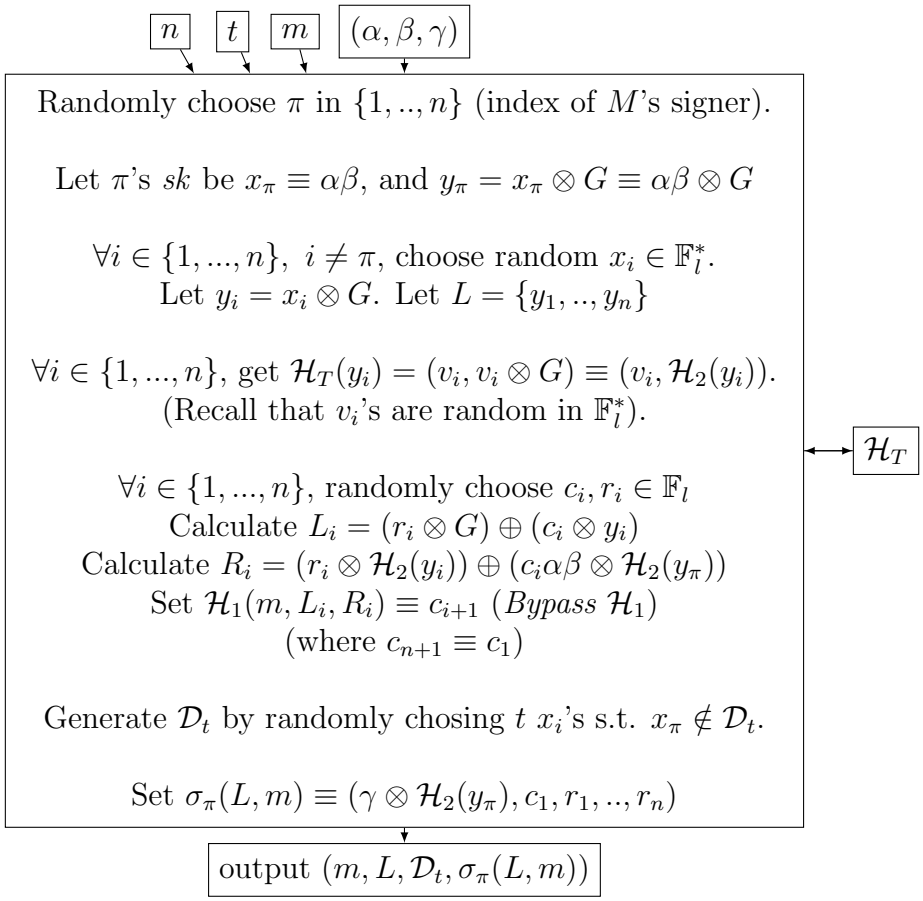
  $$P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L) \; is \; valid] > \frac{1}{n-t} + \epsilon(k)$$
  $$\text{if } x_\pi \notin \mathcal{D}_t \text{ and } 0 \leq t < n-1$$

  Recall that since $x_\pi \notin \mathcal{D}_t$, one can automatically rule out all the compromised ring members as possible signers (the logic was described in the anonymity section of part 5). One can then limit the guessing range of the identity of the signer to the uncompromised batch of $(n-t)$ remaining members.

  We now build $M \in$ PPT(k) that colludes with $\mathcal{A}(\omega)$ to solve the DDH problem. M's input consists of 1) The tuple (α, β, γ) being tested for DDH, 2) A certain ring size n (randomly chosen), 3) A number $0 \leq t < n-1$ of compromised members (randomly chosen), and 4) A message m (randomly chosen).

  M outputs a tuple consisting of 1) The message m, 2) A randomly generated ring L of size n, 3) A randomly chosen set $\mathcal{D}_t$ of t compromised secret keys, and 4) A not-necessarily valid signature $\sigma_\pi(L, m)$ assigned to ring member π s.t. $x_\pi \notin \mathcal{D}_t$.

  We let M run the following algorithm:



M feeds its output $(m, L, \mathcal{D}_t, \sigma_\pi(L, m))$ to $\mathcal{A}(\omega)$. In order for $A(\omega)$ to use its advantage in guessing the signer's identity, it must be given a valid signature (i.e., a signature that is an element of the range of acceptable signatures over all RO $\mathcal{H}_1$. For $\sigma_\pi(L, m)$ to be a valid signature, $(G, \alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ must be a DDH instance. Indeed, let $\mathcal{H}_1$ be partially defined as per the design of M. We show that for this particular $\mathcal{H}_1$, the signature obtained is an element of the range of acceptable signatures. First note that:

If $(\gamma = \alpha\beta)\ \cap\ (c'_i = c_i)\ \cap\ (L'_i = L_i)\ \cap\ (R'_i = R_i)$ then we get:

$$\{\ c'_{i+1} = \mathcal{H}_1(m, L'_i, R'_i)\ (\text{mod } l) = \mathcal{H}_1(m, L_i, R_i)\ (\text{mod } l) = c_{i+1}$$

$$\{\ L'_{i+1} \equiv (r_{i+1} \otimes G)\ \oplus\ (c'_{i+1} \otimes y_{i+1}) = (r_{i+1} \otimes G)\ \oplus\ (c_{i+1} \otimes y_{i+1}) = L_{i+1}$$

$$\{\ R'_{i+1} \equiv (r_{i+1} \otimes \mathcal{H}_2(y_{i+1}))\ \oplus\ (c'_{i+1}\gamma \otimes \mathcal{H}_2(y_\pi)) = (r_{i+1} \otimes \mathcal{H}_2(y_{i+1}))\ \oplus\ (c_{i+1}\alpha\beta \otimes \mathcal{H}_2(y_\pi)) = R_{i+1}$$

Since $(G, \alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ is a DDH instance then we necessarily have $\gamma = \alpha\beta$

Moreover, recall that $c'_1 = c_1$ (by design of $\mathcal{V}$). And so $L'_1 = L_1$ and $R'_1 = R_1$. We therefore conclude by induction on c'_i that $\forall i \in \{1, .., n+1\}$, $c'_i = c_i$. In particular, $c'_{n+1} = c_{n+1} = c_1$. This in turn implies that $\sigma_\pi(L, m)$ is a valid signature.

On the other hand, if $(G, \alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ is not a DDH instance, then $R_i \neq R'_i$ and with overwhelming probability $\sigma_\pi(L, m)$ is not a valid signature.

Recall that $\mathcal{A}(\omega)$ can send queries to $\mathcal{H}_1$ and $\mathcal{H}_T$ during execution. It is important to enforce consistency between M and $\mathcal{A}(\omega)$'s query results obtained from RO $\mathcal{H}_1$ and RO $\mathcal{H}_T$ on the same input. There are no risks of faulty collisions in so far as $\mathcal{H}_T$ is concerned (by design of M). However, M bypasses RO $\mathcal{H}_1$ and conducts its own backpatching to $\mathcal{H}_1(m, L_i, R_i),\ \forall i \in \{1, ..., n\}$. If $\exists i \in \{1, ..., n\}$ such that $\mathcal{A}(\omega)$ queries $\mathcal{H}_1$ on input (m, L_i, R_i), then with overwhelming probability, it will conflict with M's backpatched value causing the execution to halt. The aforementioned collision must be avoided. In order to do so, we first calculate the probability of its occurence. We assume that during execution, $\mathcal{A}(\omega)$ can make a maximum of Q_1 queries to RO $\mathcal{H}_1$. Q_1 is assumed to be polynomial in the security parameter k, since the adversary is modeled as a PPT Turing machine.

$$P[Col] \ = P[\cup_{i\in\{1,...,n\},\ all\ (m,L_i,R_i)}\{(m, L_i, R_i)\ appeared\ in\ M \\ and\ in\ at\ least\ one\ of\ the\ Q_1\ queries\ to\ RO\ \mathcal{H}_1\}]$$

$$\leq\ \sum_{i=1}^{n} P[\cup_{all\ L_i}\{L_i\ appeared\ in\ M\ and\ was\ part\ of\ at\ least\ one\ of \\ the\ Q_1\ queries\ to\ RO\ \mathcal{H}_1\}]$$

$$\leq \sum_{i=1}^{n}\sum_{all\ L_i\in\{G\}} P[\cup_{(j=1,..,Q_1)}\{L_i\ appeared\ in\ M\ and\ was\ part\ of\ at\ least\ the \\ j^{th}\ query\ to\ RO\ \mathcal{H}_1\}]$$

$$\leq \sum_{i=1}^{n}\sum_{all\ L_i\in\{G\}}\sum_{j=1}^{Q_1} P[L_i\ appeared\ in\ M\ and\ was\ part\ of\ at\ least\ the \\ j^{th}\ query\ to\ RO\ \mathcal{H}_1]$$

$$\leq \sum_{i=1}^{n}\sum_{all\ L_i\in\{G\}}\sum_{j=1}^{Q_1}\frac{1}{|\{G\}|^2}\ = n|\{G\}|\times\frac{Q_1}{|\{G\}|^2}\ = \frac{nQ_1}{|\{G\}|} < \frac{nQ_1}{2^k}.$$

$$(since\ k < log_2(|\{G\}^*|) < log_2(|\{G\}|)\ by\ design).$$

and so we conclude that:

$$P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[(\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi)\ \cap\ \overline{Col}\mid \sigma_\pi(m, L)\ is\ valid] =$$

$$P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L)\ is\ valid] - \\ P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[(\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi)\ \cap\ Col \mid \sigma_\pi(m, L)\ is\ valid]$$

$$> P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L)\ is\ valid]\ -\ P[Col]$$

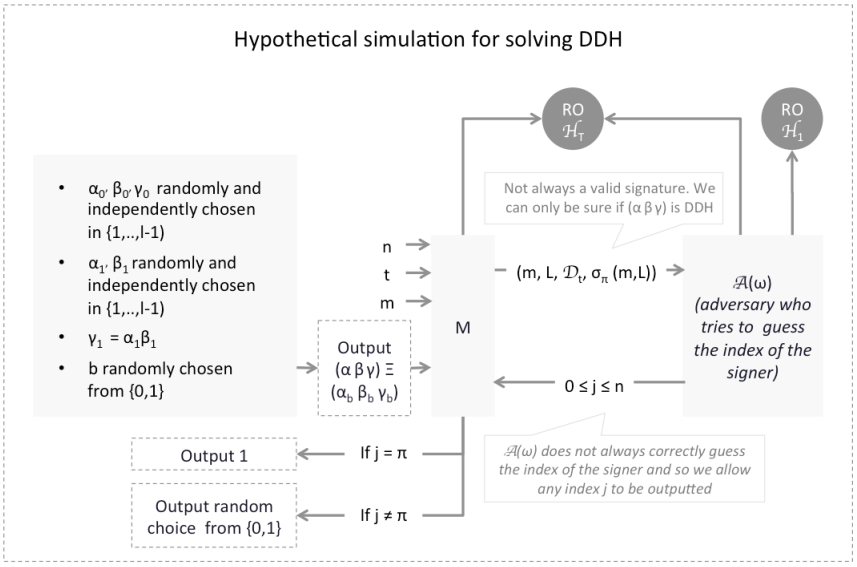
$$> P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L)\ is\ valid]\ -\ \frac{nQ_1}{2^k}$$

$$> \frac{1}{n-t} + \nu(k)$$

whenever $x_\pi \notin \mathcal{D}_t$ and $0 \leq t < n-1$. Here, $\nu(k) \equiv \epsilon(k) - \frac{nQ_1}{2^k}$ is non-negligibale in k

After execution, $\mathcal{A}(\omega)$ returns to M an integer $1 \leq j \leq n$. M then outputs 1 if $j = \pi$, or outputs 0/1 with equal probability otherwise. The following diagram

summarizes the process:



Using the setting described above, we now calculate the probability of M guessing whether $(G, \alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ is DDH or not. The calculation is the same as the one previously conducted in part 5. In what follows we make use of the following notational simplifications:

- We refer to $M(\alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ simply as M.
- We refer to $\mathcal{A}^{\mathcal{H}_1, \mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L))$ simply as $\mathcal{A}(\omega)$.

We start by noticing that

$$P[M = b] = P[M = b|b = 1] \times P[b = 1] + P[M = b|b = 0] \times P[b = 0]$$

$$= \tfrac{1}{2} \times P[M = b|b = 1] + \tfrac{1}{2} \times P[M = b|b = 0]$$

1. Case $(b = 1)$: In this case, $(G, \alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ is a DDH instance and so as we saw earlier, $\sigma_\pi(m, L)$ will be a valid signature. $\mathcal{A}(\omega)$ would then use its hypothetical advantage to guess the index of the signer among the $(n - t)$ non-compromised ring members. We get:

$$P[M = b|b = 1] \geq P[(M = b) \cap (\overline{Col}) \ |b = 1] = P[(M = b) \cap (\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \ |b = 1] + P[(M = b) \cap (\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col})|b = 1]$$

$$= P[M = b \mid (b = 1), (\mathcal{A}(\omega) = \pi), (\overline{Col})] \times P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 1)] + P[M = b \mid (b = 1), (\mathcal{A}(\omega) \neq \pi), (\overline{Col})] \times P[(\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \mid (b = 1)]$$

$$= 1 \times P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 1)] + \tfrac{1}{2} \times P[(\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \mid (b = 1)]$$

(by design of M).

Since $\sigma_\pi(m, L)$ is a valid signature, we have:

$P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 1)] > \frac{1}{n-t} + \nu(k)$, for ν non-negligible in k. Let $P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 1)] = \frac{1}{n-t} + \zeta$ for some $\zeta \geq \nu(k)$. Hence $P[(\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \mid (b = 1)] = 1 - \frac{1}{n-t} - \zeta$. We get:

$$P[M = b|b = 1] \geq 1 \times (\tfrac{1}{n-t} + \zeta) \ + \ \tfrac{1}{2} \times (1 - \tfrac{1}{n-t} - \zeta)$$

$$= \ \tfrac{1}{2} + \tfrac{1}{2(n-t)} + \tfrac{\zeta}{2} \ \geq \ \tfrac{1}{2} + \tfrac{1}{2(n-t)} + \tfrac{\nu(k)}{2}$$

2. Case $(b = 0)$: In this case, we do not know if $(G, \alpha \otimes G, \beta \otimes G, \gamma \otimes G)$ is a DDH instance or not, and hence can not be sure whether $\sigma_\pi(m, L)$ is a valid signature. Consequently, $\mathcal{A}(\omega)$ can no longer use its advantage in guessing the index of the signer, because this advantage works only when it is fed a valid signature. We get:

$$P[M = b|b = 0] \geq P[(M = b) \cap (\overline{Col}) \ |b = 0] = P[(M = b) \cap (\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \ |b = 0] + \ P[(M = b) \cap (\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \ |b = 0]$$

$$= P[M = b \mid (b = 0), (\mathcal{A}(\omega) = \pi), (\overline{Col})] \times P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 0)] + P[M = b \mid (b = 0), (\mathcal{A}(\omega) \neq \pi), (\overline{Col})] \times P[(\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \mid (b = 0)]$$

$$= 0 \times P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 0)] + \tfrac{1}{2} \times P[(\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \mid (b = 0)]$$

(by design of M).

and since $\mathcal{A}(\omega)$ can no longer use its advantage to guess the index of the signer, the best thing it can do is random guessing among non-compromised members. Hence $P[(\mathcal{A}(\omega) = \pi) \cap (\overline{Col}) \mid (b = 0)] = \frac{1}{n-t}$, and $P[(\mathcal{A}(\omega) \neq \pi) \cap (\overline{Col}) \mid (b = 0)] = 1 - \frac{1}{n-t}$. We get:

$$P[M = b|b = 0] \geq 0 \times (\tfrac{1}{n-t}) \ + \ \tfrac{1}{2} \times (1 - \tfrac{1}{n-t}) = \ \tfrac{1}{2} - \tfrac{1}{2(n-t)}$$

Putting it altogether, we conclude that:

$$P[M = b] \geq \tfrac{1}{2} \times (\tfrac{1}{2} + \tfrac{1}{2(n-t)} + \tfrac{\nu(k)}{2}) + \tfrac{1}{2} \times (\tfrac{1}{2} - \tfrac{1}{2(n-t)}) = \tfrac{1}{2} + \tfrac{\nu(k)}{4}$$

Since $\nu(k)$ is non-negligible in k, the above probability outperforms random guessing. This contradicts the intractability of DDH. Similarly, we can show $P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi] \mid \sigma_\pi(m, L)$ *is valid*] is also bounded from below. We finally conclude that for any polynomial $Q(k)$:

$$\tfrac{1}{n-t} - \tfrac{1}{Q(k)} \leq P_{\omega,\mathcal{H}_1,\mathcal{H}_T}[\mathcal{A}^{\mathcal{H}_1,\mathcal{H}_T}(\omega)(m, L, \mathcal{D}_t, \sigma_\pi(m, L)) = \pi \mid \sigma_\pi(m, L) \textit{ is valid}] \leq \tfrac{1}{n-t} + \tfrac{1}{Q(k)}, \text{ if } x_\pi \notin \mathcal{D}_t \text{ and } 0 \leq t < n - 1.$$

- Case 2: $x_\pi \notin \mathcal{D}_t$ and $t = n - 1$.

In this case, $\mathcal{A}(\omega)$ can check if I_π (the key-image or tag of $\sigma_\pi(m, L)$) matches any of the compromised tags $\hat{x}_i \otimes \mathcal{H}_2(\hat{x}_i \otimes G)$, for $i \in \{1, .., t = (n - 1)\}$. With

overwhelming probability, none of them will match since we proved that the scheme is exculpable and so no one can forge a signature with a tag of a non-compromised member. Proceeding by elimination, $\mathcal{A}(\omega)$ can then conclude that the signer is π.

- Case 3: $x_\pi \in \mathcal{D}_t$.

  In this case, $\mathcal{A}(\omega)$ can check which of the compromised tags $\hat{x}_i \otimes \mathcal{H}_2(\hat{x}_i \otimes G)$ $(i \in \{1, .., t\})$ matches I_π (the key-image or tag of $\sigma_\pi(m, L)$). Only one of them will match (due to exculpability), subsequently revealing the identity of the signer.

7 Security analysis - Linkability

Recall that the *linkability* property means that if a secret key is used to issue more than one signature, then the resulting signatures will be linked and flagged by $\mathcal{L}$ (the linkability algorithm).

We proved in part 5 of this series that a signature scheme is linkable if and only if $\forall n \in \{1, .., l-1\}, \forall L \equiv \{y_1, .., y_n\}$ a ring of n members, it is not possible to produce $(n+1)$ valid signatures with pairwise different key-images such that all of them get labeled *independent* by $\mathcal{L}$.

To prove that the LSAG scheme is linkable we follow a *reductio ad absurdum* approach, similar to the one described in part 5 of this series:

- Assume that the LSAG scheme is not linkable.
- The equivalence above would imply that $\exists L \equiv \{y_1, .., y_n\}$ such that it can produce $(n+1)$ valid signatures with pairwise different key-images (i.e.,$\forall i, j \in \{1, .., n\}, i \neq j \Rightarrow (I_i \equiv x_i \otimes \mathcal{H}_2(y_i)) \neq (I_j \equiv x_j \otimes \mathcal{H}_2(y_j))$), and such that all of them get labeled *independent* by $\mathcal{L}$.
- This means that there must exist a signature (from the set of $(n+1)$ valid signatures) with key-image I_δ such that $\forall i \in \{1, .., n\},\ I_\delta \neq I_i \equiv x_i \otimes \mathcal{H}_2(y_i)$. Denote this signature by $\sigma_\delta \equiv (I_\delta, c_1, r_1, .., r_n)$.
- When verifying the validity of $\sigma_\delta,\ \mathcal{V}$ will first compute the following:
  - $c'_1 \equiv c_1$
  - for all $i \in \{1, .., n\}$:
    $\{\ L'_i = (r_i \otimes G) \oplus (c'_i \otimes y_i)$
    $\{\ R'_i = (r_i \otimes \mathcal{H}_2(y_i)) \oplus (c'_i \otimes I_\delta)$
    $\{\ c'_{i+1} = \mathcal{H}_1(m, L'_i, R'_i)$
- $\forall i \in \{1, .., n\}$, the system of 2 equations given by L'_i and R'_i can be equivalently written as:

$$\{\ r_i + c'_i x_i = log_G(L'_i)$$
$$\{\ r_i \otimes \mathcal{H}_2(y_i)) \oplus (c'_i \otimes I_\delta) = R'_i$$

For a given L'_i, R'_i, and $i \in \{1, .., n\}$, this constitutes a system of 2 equations in variables r_i and c'_i.

- Since $\forall i \in \{1, .., n\},\ I_\delta \neq x_i \otimes \mathcal{H}_2(y_i)$, the system of 2 equations corresponding to each i is independent and admits a unique solution $(r_i^*, (c'_i)^*)$ for any given L'_i, and R'_i. In particular, that means that the value $c'_1 \equiv c_1$ is well defined and equal to $(c'_1)^*$.
- By virtue of being a valid signature, σ_δ must satisfy $\mathcal{V}$'s verification equation. More specifically, it must be that $c_1 = \mathcal{H}_1(m, L'_n, R'_n) \pmod l$. But RO $\mathcal{H}_1$ is random by definition. The probability that it outputs a specific value is eqal to $\frac{1}{q}$ (recall that the range of $\mathcal{H}_1 = \mathbb{F}_q$). Since by design we have $2^k < l - 1 < l < q$, we conclude that the probability that $\mathcal{H}_1(m, L'_n, R'_n) \pmod l = (c'_1)^*$ is upper-bounded by $\frac{1}{2^k}$ and is hence negligible. In other terms, the probability that σ_δ is a valid signature is negligible.

We can then conclude that with overwhelming probability, the ring $L \equiv \{y_1, .., y_n\}$ can not produce $(n + 1)$ valid signatures with pairwise different key-images and such that all of them get labeled *independent* by $\mathcal{L}$. The LSAG scheme as we introdued it is hence linkable.

References

[1] A. Back. Ring signature efficiency. https://bit.ly/2GIQ6Ag, 2015.

[2] E. Fujisaki and K. Suzuki. Traceable ring signatures. *Public Key Cryptography*, pages 181–200, 2007.

[3] J. K. Liu, V. K. Wei, and D. S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups. *ACISP*, Lecture Notes in Computer Science(3108):325–335, 2004.

[4] S. Noether and A. Mackenzie. Ring confidential transactions. *Monero Research Lab*, 2016.